Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	
Use of Spectrum Bands Above 24 GHz For Mobile Radio Services	GN Docket No. 14-177
Establishing a More Flexible Framework to Facilitate Satellite Operations in the 27.5-28.35 GHz and 37.5-40 GHz Bands	IB Docket No. 15-256
Petition for Rulemaking of the Fixed Wireless Communications Coalition to Create Service Rules for the 42-43.5 GHz Band	RM-11664
Amendment of Parts 1, 22, 24, 27, 74, 80, 90, 95, and 101 To Establish Uniform License Renewal, Discontinuance of Operation, and Geographic Partitioning and Spectrum Disaggregation Rules and Policies for Certain Wireless Radio Services	WT Docket No. 10-112
Allocation and Designation of Spectrum for Fixed-Satellite Services in the 37.5-38.5 GHz, 40.5-41.5 GHz and 48.2-50.2 GHz Frequency Bands; Allocation of Spectrum to Upgrade Fixed and Mobile Allocations in the 40.5-42.5 GHz Frequency Band; Allocation of Spectrum in the 46.9-47.0 GHz Frequency Band for Wireless Services; and Allocation of Spectrum in the 37.0-38.0 GHz and 40.0-40.5 GHz for Government Operations	IB Docket No. 97-95

PETITION FOR PARTIAL RECONSIDERATION OF NCTA – THE INTERNET & TELEVISION ASSOCIATION

Rick Chessen
Danielle J. Piñeres
NCTA – The Internet & Television Association
25 Massachusetts Avenue, NW – Suite 100
Washington, DC 20001-1431
(202) 222-2445

December 14, 2016

NCTA – The Internet & Television Association (NCTA) appreciates the Commission's forward-thinking efforts to make millimeter wave spectrum bands available for next-generation 5G technologies. Overall, the rules adopted by the Commission—which appropriately emphasize the need for a balance of licensed and unlicensed 5G spectrum—will promote 5G innovation and the deployment of state-of-the-art, next-generation networks. However, pursuant to section 1.429 of the Commission's rules,[1] NCTA hereby petitions for reconsideration of one narrow aspect of the Commission's 5G Order: the cybersecurity reporting requirement. Specifically, NCTA requests that the Commission reconsider the adoption of 47 C.F.R. § 30.8, which would require Upper Microwave Flexible Use Service (UMFUS) licensees to file a public statement, signed by a senior executive, describing their cybersecurity practices.

NCTA strongly supports public-private efforts to combat cybersecurity threats. But requiring licensees to file public statements about the cybersecurity of their networks would significantly undermine industry's investment in and integration of leading and innovative cybersecurity practices in 5G deployments. The rule is an unnecessary regulatory intervention that would impose substantial compliance costs on 5G network operators with no meaningful corresponding benefit in light of the fact that network providers already have enormous incentives to adopt measures to protect their networks. Preparing the public statement required by the Commission would involve a company's technical, engineering, and operations teams and would need to be reviewed by legal counsel before a corporate officer could sign. Moreover, the rule would have the unintended consequence of increasing—not decreasing—security threats to 5G deployments. Standards bodies and other industry-led forums are best positioned to ensure

---

[1] 47 C.F.R. § 1.429(a).

5G network security; the Commission need not intervene with new reporting obligations that may undermine security and will impose an unnecessary burden.

Furthermore, as a procedural matter, the Commission adopted this rule without adequate notice or opportunity to comment. The proposed rule text did not appear in the Commission's Notice of Proposed Rulemaking (NPRM), which asked general questions about 5G network security, but did not propose or even inquire about a cybersecurity reporting requirement.

The Commission should also reconsider the cybersecurity reporting rule because the record does not support its adoption. To the contrary, the record establishes that industry, working within a variety of industry-led forums, is already working hard to ensure the security of future 5G networks. The Commission's conclusion that network operators should file public reports with the Commission on their network security plans simply because "5G services will need to be highly secure prior to deployment" is unsupported.[2] For these reasons, NCTA urges the Commission to reconsider this one aspect of its broader 5G Order.

I. INDUSTRY-LED APPROACHES, NOT A COMMISSION-IMPOSED REPORTING REQUIREMENT, BEST PROMOTE 5G NETWORK SECURITY

Section 30.8 requires 5G network operators to describe publicly their cybersecurity plans for protecting their UMFUS networks. This requirement is more likely to expose 5G networks to cybersecurity threats than help the Commission to ensure their protection. Even the high-level information that the rule requires UMFUS licensees to disclose may unintentionally reveal a vulnerability that bad actors could exploit. On the other hand, if the public information

---

[2] *Use of Spectrum Bands Above 24 GHz for Mobile Radio Services, et al.*, Report and Order and Further Notice of Proposed Rulemaking, 31 FCC Rcd 8014, 8103-04 ¶ 261 (2016) (*5G Order*).

submitted by network operators is truly so generic and high-level as to thwart would-be exploiters, that information would be of such limited utility to the Commission in evaluating whether licensees have in fact "engage[d] in the development of security measures at an earlier stage" or in "identifying security risks, including areas where more attention to security may be needed"[3] that it does not justify the burden of imposing new reporting requirements. For these reasons, it should come as no surprise that the record developed since the Commission adopted section 30.8 clearly opposes this ill-considered requirement.[4]

To comply with the rule, UMFUS licensees would incur substantial costs. A network operator's technical, engineering, and operations teams would all be involved in preparing a statement regarding cybersecurity practices, and the statement would also need to be reviewed by legal counsel before a corporate officer could sign. Furthermore, a band-by-band approach to cybersecurity, should the Commission impose cybersecurity requirements in other bands, would increase compliance costs. Network operators use a variety of spectrum bands to optimize their networks and best meet customers' needs and their costs of compliance would multiply if cybersecurity requirements varied among those different spectrum bands. The Commission has failed to show that the benefits of the statement, which would significantly expand a company's regulatory risk and legal exposure, would exceed these costs to network operators.

---

3 *Id.* at 8104 ¶ 262.

4 Comments of AT&T, GN Docket No. 14-177, IB Docket Nos. 15-256 & 97-95, RM-11664, and WT Docket No. 10-112, at 14-16 (filed Sept. 30, 2016) (AT&T Comments); Comments of CTIA, GN Docket No. 14-177, IB Docket Nos. 15-256 & 97-95, RM-11664, and WT Docket No. 10-112, at 10-11 & n.28 (filed Sept. 30, 2016) (CTIA Comments).

Moreover, even if the type of reporting contemplated by the new rule could somehow advance security, the Commission is not the appropriate entity to address network security. As Commissioner Pai noted in his separate statement issued with the 5G Order, the Commission "lack[s] the expertise and authority to dive headlong into this issue, and . . . [no] agency should take a band-by-band approach to cyber. These are issues that are better left for security experts to handle in a more comprehensive way."[5] In fact, security experts are already hard at work on these issues—commenters in this proceeding noted that the mobile industry is actively engaged in the development of appropriate cybersecurity protections.[6] Moreover, many industry-led forums—including the National Institute of Science and Technology (which developed and continues to refine the Cybersecurity Framework), the Commission's Communications Security, Reliability and Interoperability Council (CSRIC), and the Communications Sector Coordinating Council as part of the public-private partnership with federal government partners such as the Department of Homeland Security and the Commission—already exist to address best practices

---

5 *5G Order*, 31 FCC Rcd at 8279 (Statement of Commissioner Ajit Pai); *see also id.* at 8282 (Statement of Commissioner Michael O'Rielly) ("I don't think that this reporting requirement is necessary or all that helpful. Once again, this is the Commission gathering data for the purposes of monitoring, but it is really a means for the Commission to interfere in the design and operations of networks and the starting point for future regulation.").

6 *See, e.g.*, Comments of the Telecommunications Industry Association, GN Docket No. 14-177, IB Docket Nos. 15-256 & 97-95, RM-11664, and WT Docket No. 10-112, at 36 (filed Jan. 27, 2016) (TIA Comments) ("TIA's members are actively engaged in a wide range of efforts to assure that network and device security is preserved to the maximum extent feasible."); Comments of 4G Americas, GN Docket No. 14-177, IB Docket Nos. 15-256 & 97-95, RM-11664, and WT Docket No. 10-112, at 18 (filed Jan. 26, 2016) (4G Americas Comments) ("4G Americas assures the Commission that its members are exploring means to ensure the integrity of each data object in 5G networks.").

and share information regarding cyber threats to mobile networks.[7] The Commission's 5G reporting requirement is out of sync with existing industry/government mechanisms to address a fast-changing cyber threat landscape and would detract from these efforts in other forums.

II. THE COMMISSION ADOPTED THE CYBERSECURITY REPORTING REQUIREMENT WITHOUT ADEQUATE NOTICE AND OPPORTUNITY TO COMMENT

The Commission should reconsider its adoption of the 5G reporting requirement because it did not afford interested parties adequate notice of the proposed rule or a meaningful opportunity to comment. In the section of the NPRM that deals with security issues, the Commission merely sought "comment on how to ensure that effective security features are built into key design principles for all mmW band communications devices and networks,"[8] and posed a series of questions about confidentiality, integrity, and availability of 5G networks.[9] The Commission did not so much as hint that it was considering a new public reporting requirement,

---

7 *See, e.g.*, U.S. Dep't of Commerce, Nat'l Inst. of Standards & Tech., *Framework for Improving Critical Infrastructure Cybersecurity*, at 1 (Feb. 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (describing how the NIST framework "us[es] business drivers to guide cybersecurity activities" and provides "a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors"); FCC, *Communications Security, Reliability and Interoperability Council V*, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability; The Communications Security, Reliability and Interoperability Council IV, *Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report*, at 31 (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_ Final_Report_031815.pdf (recommending that the Commission "promote the voluntary use of the NIST CSF among all communications sector members"); U.S. Commc'ns Sector Coordinating Council, *FAQ: Why Should My Business Join the CSCC?*, http://www.comms-scc.org/faq/.

8 *Use of Spectrum Bands Above 24 GHz for Mobile Radio Services, et al.*, Notice of Proposed Rulemaking, 30 FCC Rcd 11,878, 11,952-53 ¶ 261 (2015).

9 *Id.* at 11,952-53 ¶¶ 261-65.

much less tee up the specific text of section 30.8 in its proposed rules.[10] Consequently, commenters focused on 5G cybersecurity issues generally and had no opportunity to address the specific pitfalls of a Commission mandate to file a public description of a network operator's cybersecurity plans.

After the deadline for reply comments, the Commission changed its proposal. Just two weeks before the sunshine period prevented further advocacy about the NPRM, the Commission issued a fact sheet that proposed a network security reporting requirement for the first time.[11] That late-breaking announcement, which the 5G Order never mentions, could not cure the NPRM's Administrative Procedure Act (APA) defects.[12] Nor did it accurately describe the rule the Commission ultimately adopted. The fact sheet failed, for example, to mention that the Commission intended to require a public statement or to set forth the details of what the report must contain. After seeing the fact sheet and the rule, industry's reaction has been uniformly negative.[13] Clearly, the Commission adopted the rule without the benefit of that feedback; none

---

[10] *See generally id.* at 11,978-96 (Appendix A).

[11] *See* FCC, *Fact Sheet: Spectrum Frontiers Proposal to Identify, Open Up Vast Amounts of New High-Band Spectrum for Next Generation (5G) Wireless Broadband* (Jun. 23, 2016), https://apps.fcc.gov/edocs_public/attachmatch/DOC-339990A1.pdf.

[12] 5 U.S.C. § 553(b)(3) (stating that an NPRM "shall include . . . either the terms or substance of the proposed rule or a description of the subjects and issues involved"); *Small Refiner Lead Phase-Down Task Force v. U.S. Envtl. Prot. Agency*, 705 F.2d 506, 549 (D.C. Cir. 1983) ("Agency notice must describe the range of alternatives being considered with reasonable specificity. Otherwise, interested parties will not know what to comment on, and notice will not lead to better-informed agency decisionmaking.").

[13] AT&T Comments at 14-16; CTIA Comments at 10-11 & n.28; Letter from Rebecca Murphy Thompson, EVP & General Counsel, Competitive Carriers Association, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 14-177, at 6 (filed July 7, 2016) (describing conversation regarding cybersecurity with legal advisors to Commissioners Rosenworcel and O'Rielly); *see also* Letter from Charla M. Rath, Vice President – Wireless Policy

of the criticism parties were able to provide before the sunshine period is addressed in the 5G Order. This lack of transparency falls far short of APA notice and comment requirements—and basic due process guarantees.

III. THE RECORD DOES NOT SUPPORT ADOPTING A CYBERSECURITY REPORTING REQUIREMENT

In adopting section 30.8, the Commission relied on comments that highlighted the importance of ensuring security by design. But the 5G Order does not identify a single commenter that suggested the reporting requirement that the Commission adopted—because no commenter expressed support for such a reporting structure on the record. Nonetheless, and without further reasoning, the Commission concluded that because 5G networks need to be secure by design, "it [is] reasonable that the Commission be apprised of security plans in place prior to 5G services becoming operational."[14] But there is no reasonable fit between the goal of fostering more secure 5G networks and devices and the Commission's chosen mechanism of requiring private companies to publicly report their security protocols, tools, and measures. Further, the imposition of a compulsory and open-ended reporting requirement on "security plans" is antithetical to the wide range of initiatives—taking place at other government agencies such as the Department of Homeland Security, the National Institute of Standards and Technology, the National Telecommunications and Information Administration, and the Federal Trade Commission, as well as in multi-stakeholder industry groups like the Broadband Internet

---

Development, Verizon, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 14-177, at 2 (filed July 7, 2016).

[14] *5G Orde*r, 31 FCC Rcd at 8103-04 ¶ 261.

Technical Advisory Group (BITAG)—aimed at promoting voluntary measures and best practices for securing next-generation networks and attendant connected devices.

As AT&T has pointed out, comments acknowledging industry's focus on "security-by-design and ensuring the well-being of end-users in complex digital domains" can hardly be viewed as justification for a prescriptive cybersecurity *reporting* rule that itself raises security concerns.[15] 5G Americas—which the Commission cites for the proposition "that security should be a fundamental component in the design of any new network architecture and protocols"[16]—noted that *industry-developed* 5G standards could help to ensure the security of 5G networks, but in no way suggested that the Commission should regulate in this space.[17] Similarly, Huawei—also heavily cited by the Commission in its discussion of the need for cybersecurity regulations[18]—emphasized "research and standards-related efforts" and the importance of multistakeholder collaboration in developing 5G cybersecurity solutions.[19]

The Commission also did not acknowledge that most commenters addressing cybersecurity issues on the record cautioned against Commission-imposed cybersecurity requirements and highlighted the importance of industry-driven solutions. For instance, the Telecommunications Industry Association stated that "it would be ill-advised for the Commission to adopt new mmW-specific security rules in this proceeding. Indeed, marketplace

---

15 AT&T Comments at 15.

16 *5G Order*, 31 FCC Rcd at 8103 ¶ 261.

17 4G Americas Comments at 17-18.

18 *5G Order*, 31 FCC Rcd at 8103 ¶ 260.

19 Comments of Huawei Technologies, Inc. (USA) and Huawei Technologies Co., Ltd., GN Docket No. 14-177, IB Docket Nos. 15-256 & 97-95, RM-11664, and WT Docket No. 10-112, at 24 (filed Jan. 28, 2016).

forces and existing private sector and government efforts will lead service providers and device manufacturers to build into their offerings the security features that consumers demand."[20] Similarly, EchoStar noted that it "appreciates the Commission's concern with security, but submits that there is no concern with respect to FSS operations that needs to be addressed."[21]

Because the record does not support the adoption of a Commission-imposed cybersecurity reporting requirement, the Commission should reconsider this one aspect of its decision.[22]

IV. CONCLUSION

Without the benefit of meaningful industry comment, and without adequate notice, the Commission has adopted a cybersecurity reporting requirement that will do more harm than good. Rather than requiring UMFUS licensees to file public plans that themselves create new vulnerabilities, the Commission should allow industry organizations to continue their ongoing work, including public-private cooperation in more appropriate contexts, to secure 5G networks.

---

[20] TIA Comments at 37; *see also* Comments of Straight Path Communications, Inc., GN Docket No. 14-177, IB Docket Nos. 15-256 & 97-95, RM-11664, and WT Docket No. 10-112, at 39 (filed Jan. 27, 2016) ("Straight Path opposes the imposition of any such security requirements. While Straight Path appreciates and shares the Commission's concern for security, imposition of these obligations is inconsistent with Commission practice and contrary to the public interest.").

[21] Comments of EchoStar Satellite Operating Corporation, Hughes Network Systems, LLC, and Alta Wireless, Inc., GN Docket No. 14-177, IB Docket Nos. 15-256 & 97-95, RM-11664, and WT Docket No. 10-112, at 41 (filed Jan. 27, 2016).

[22] *See Motor Vehicle Mfrs. Ass'n of the U.S. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983) ("Normally, an agency rule would be arbitrary and capricious if the agency has . . . offered an explanation for its decision that runs counter to the evidence before the agency, or is so implausible that it could not be ascribed to a difference in view or the product of agency expertise."); *Gen. Chem. Corp. v. United States*, 817 F.2d 844, 849 (D.C. Cir. 1987) (stating that an agency must "engage[] in reasoned decisionmaking that is both adequately explained, and supported by substantial evidence in the record as a whole").

NCTA respectfully requests that the Commission reconsider and reverse this substantively and procedurally flawed requirement.

Respectfully submitted,

/s/ Rick Chessen

_____

Rick Chessen
Danielle J. Piñeres
NCTA – The Internet & Television Association
25 Massachusetts Avenue, NW – Suite 100
Washington, DC 20001-1431
(202) 222-2445

December 14, 2016